IN THE UNITED STATE PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re application of:	**Antonius Adrianus Kalker et al.**
For:	**WATERMARK EMBEDDING AND DETECTION**
Serial No.	**10/564,421**
Filed	**January 11, 2006**
Art Unit	**4148**
Examiner	**Travis D. Pogmore**
Attorney Docket No.	**NL030808US1**
Confirmation No.	**8966**

APPEAL BRIEF

ON APPEAL FROM GROUP ART UNIT 4148

Mail Stop Appeal Brief Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

This Appeal Brief is submitted both in support of the Notice of Appeal, which was filed April 21, 2009, and in response to the Final Office Action dated January 21, 2009. The two-month period for filing this Appeal Brief expires on June 22, 2009, because June 21, 2009 falls on a Sunday.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The real party in interest is Koninklijke Philips Electronics N.V., the assignee of record, whose three-page assignment was recorded on January 11, 2006 in the USPTO beginning at Reel 017473, Frame 0978.

II. RELATED APPEALS AND INTERFERENCES

Appellants are not aware of any pending appeals, judicial proceedings, or interferences which may be related to, directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

a) Claims 1-3 and 5-15 are pending, stand rejected, and are the subject of this appeal.

b) Claims 1, 9, 14, and 15 are all independent claims.

c) Claims 4 and 16 have been cancelled by a prior response of record in this application.

IV. STATUS OF AMENDMENTS

The claims listed in Section VIII, Claims Appendix, of this Appeal Brief correspond to the claims as submitted in Appellants' response filed December 3, 2008. All amendments filed in this application have been entered and there are no amendments pending.

V. SUMMARY OF CLAIMED SUBJECT MATTER

It should be explicitly noted that it is not the Appellants' intention that the currently claimed or described embodiments be limited solely to operation within the illustrative embodiments identified below. Furthermore, descriptions of illustrative embodiments are provided below in association with portions of the claims, which are related to the identified illustrative embodiments, entirely for compliance with, and satisfaction of, the requirements for filing this appeal. There is no intention to read any further interpreted limitations into the claims as presented.

The claimed invention, as recited in claim 1, is directed to a method of embedding a digital watermark in an information signal *(page 2, lines 1-2)*; the method comprising deriving a watermark

secret from an identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert *(page 2, lines 3 and 8-9 and page 4, lines 26-32)*; embedding a digital watermark in the information signal where said embedding is controlled by the watermark secret *(page 2, lines 4-5 and page 4, lines 26-32)*; calculating a digital fingerprint from the information signal *(page 2, line 6)*; storing the calculated digital fingerprint as a reference digital fingerprint and storing, in relation to the reference digital fingerprint, said identifier data item *(page 2, lines 7-8)*.

The claimed invention, as recited in claim 9, is directed to a method of detecting a digital watermark in an information signal *(page 5, lines 14-15)*; the method comprising providing a plurality of digital reference fingerprints each calculated from a respective reference information signal, where each digital fingerprint is associated with a corresponding watermark secret *(page 5, lines 16-18)*; calculating a digital fingerprint from the information signal *(page 5, line 19)*; determining a matching digital fingerprint from the plurality of digital reference fingerprints as corresponding to the calculated digital fingerprint *(page 5, lines 20-21)*; detecting whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal *(page 5, lines 22-23)*.

The claimed invention, as recited in claim 14, is directed to an arrangement for embedding a digital watermark in an information signal *(page 6, lines 23-24 and page 4, lines 26-32)*; the arrangement comprising means for deriving a watermark secret from an identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert *(page 2, lines 3 and 8-9)*; means for embedding a digital watermark in the information signal where said embedding is controlled by a watermark secret *(page 6, lines 25-26)*; means for calculating a digital fingerprint from the information signal *(page 6, line 27)*; and means for storing the calculated digital fingerprint as a reference digital fingerprint and for storing, in relation to the reference digital fingerprint, a identifier data item from which the watermark secret can be derived *(page 6, lines 28-30)*.

The claimed invention, as recited in claim 15, is directed to an arrangement for detecting a digital watermark in an information signal *(page 6, lines 31-32)*; the arrangement comprising means for providing a plurality of digital reference fingerprints each calculated from a respective reference information signal, where each digital fingerprint is associated with a corresponding watermark

secret *(page 7, lines 1-3)*; means for calculating a digital fingerprint from the information signal *(page 7, line 4)*; means for determining a matching digital fingerprint from the plurality of digital reference fingerprints as corresponding to the calculated digital fingerprint *(page 7, lines 5-6)*; and means for detecting whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal *(page 7, lines 8-9)*.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

In the grounds of rejection to be reviewed on appeal, certain references have been cited and applied against the claims. These references are listed as follows: an article by G. Depovere et al. entitled "*Secret key watermarking with changing keys*", pp. 427-9 published by the IEEE on September 10, 2000 (hereinafter "*Depovere*"); U.S. Patent Application Publication No. 2002/0028000 to Conwell et al. (hereinafter "*Conwell*"); and U.S. Patent 5,724,425 to Chang et al. (hereinafter "*Chang*").

The grounds of rejection to be reviewed on appeal are stated below in an enumerated listing as follows:

1. Whether claims 1-3, 5-8, and 14 are properly rejected by the Office under 35 U.S.C. §103 as being unpatentable over Depovere in view of Conwell and further in view of Chang; and
2. Whether claims 9-13 and 15 are properly rejected by the Office under 35 U.S.C. §103 as being unpatentable over Conwell in view of Depovere.

VII. ARGUMENT

Appellant respectfully traverses the rejections in accordance with the detailed arguments set forth below.

1. CLAIMS 1-3, 5-8, AND 14 ARE IMPROPERLY REJECTED UNDER 35 U.S.C. §103 AS BEING UNPATENTABLE OVER DEPOVERE IN VIEW OF CONWELL AND FURTHER IN VIEW OF CHANG

Claim 1 is an independent method claim. Claims 2-3 and 5-8 depend ultimately from claim 1. Claim 14 is an independent apparatus claim that includes limitations substantially similar to those found in claim 1.

Claim 1

Claim 1 is an independent method claim that calls for:

> *A method of embedding a digital watermark in an information signal; the method comprising*
>
> - *deriving a watermark secret from an identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert;*
> - *embedding a digital watermark in the information signal where said embedding is controlled by the watermark secret;*
> - *calculating a digital fingerprint from the information signal;*
> - *storing the calculated digital fingerprint as a reference digital fingerprint and storing, in relation to the reference digital fingerprint, said identifier data item.*

Depovere appears to disclose a device for embedding a watermark payload P_1 into an information signal X_1, wherein one or more secret key patterns $S_1,\ldots, S_n$ are utilized for embedding the payload P_1 into the information signal X_1. *See Depovere in Figure 4 and in Section 3 at pages 428-9.* In Depovere, the secret key patterns $S_1, \ldots S_n$ are not constant over time and they depend on a robust signature. According to Depovere, the robust signature corresponds, via a mapping, to one of the secret key patterns $S_1, \ldots S_n$. *Ibid.* Moreover, the robust features of the information signal X_1 are combined by some technique to form the robust signature.

It has been admitted on page 4 in the present Office Action that Depovere does not teach, show, or suggest the limitations of "calculating a digital fingerprint from the information signal", "storing the calculated fingerprint as a reference digital fingerprint", "storing, in relation to the reference digital fingerprint, said identifier data item", and wherein the watermark secret is derived "by a function which is computationally hard or infeasible to invert". In order to cure these defects in Depovere, the present Office Action has applied Conwell and Chang. But Conwell and Chang do not teach, show, or suggest these limitations and do not cure the defects noted with respect to Depovere.

Conwell appears to teach that fingerprint data obtained from some information content can be used as an identifier. *See Abstract of Conwell.* This fingerprint is used as part of an identification process to trigger a response, such as performing a database lookup of the complete content related

to the fingerprint-based identification, which, in turn, leads to a number of possible applications. *See Conwell at paragraph [0030], for example.*

It is admitted on page 4 of the present Office Action that Conwell fails to teach the claimed limitation of wherein the "identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert". Contrary to the assertions in the present Office Action, it is submitted that Conwell also fails to teach, show, or suggest "storing, in relation to the reference digital fingerprint, said identifier item", wherein "the calculated digital fingerprint [is stored] as the reference digital fingerprint", and is used for "deriving the watermark secret", all as defined in claim 1.

As defined in claim 1, the identifier data item is additional data that is stored with the reference fingerprint. That is, claim 1 defines the reference fingerprint and the identifier data that are both stored. Conwell appears to suggest the storage of a fingerprint generated from attributes of the content. *See Conwell at paragraphs [0009], [0018]-[0019], and [0023]-[0025].* Nowhere in the cited section or anywhere else in the reference does Conwell teach, show, or suggest storing any identifier data in addition to the reference fingerprint. For this reason, Conwell fails to teach, show, or suggest "storing, in relation to the reference digital fingerprint, said identifier data item", as defined in claim 1. Moreover, Conwell in combination with Depovere fails to teach, show, or suggest "storing, in relation to the reference digital fingerprint, said identifier data item", as defined in claim 1. Conwell does not cure the defects from the teachings of Depovere.

Even if it were assumed, solely for the sake of argument herein, that Conwell stores additional identifier data with the reference fingerprint, Conwell lacks even a remote suggestion that such additional identifier data, if it were to exist in Conwell, is used to derive a watermark secret, as defined in claim 1. Conwell fails to teach, show, or suggest "deriving a watermark secret from an identifier data item", as defined in claim 1. Moreover, Conwell in combination with Depovere fails to teach, show, or suggest "deriving a watermark secret from an identifier data item", as defined in claim 1. Conwell does not cure the defects from the teachings of Depovere.

Chang was added to Depovere and Conwell because it was admitted that Depovere and Conwell both lack any teachings about the "identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert". Even if Chang is assumed, for the sake of argument herein, to teach the concept of computational infeasibility in the encryption art for

public key encryption algorithms, there is no teaching, showing, or suggestion in Chang that would cure the defects noted above in the teachings of Depovere and Conwell. Chang lacks any teaching, showing, or suggestion concerning "deriving a watermark secret from an identifier data item", "storing, in relation to the reference digital fingerprint, said identifier data item", and "identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert", all as defined in claim 1. Chang does not cure the defects from the teachings of Depovere and Conwell. Chang in combination with Depovere and Conwell fails to teach, show, or suggest the limitations discussed immediately above from claim 1.

For all the reasons set forth above, it is believed that the elements of claim 1 are not taught, shown, or suggested by Depovere, Conwell, and Chang, either separately or in combination. It is therefore submitted that the elements of claim 1 would not have been obvious to a person of ordinary skill in the art upon a reading of Depovere, Conwell, and Chang, separately or in combination. Thus, it is submitted that claim 1 is allowable under 35 U.S.C. §103. It is respectfully requested that the Board reverse this rejection of claim 1.

Dependent Claims 2, 3, and 5-8

Claims 2-3 and 5-8 depend either directly or indirectly upon claim 1. Each dependent claim includes all the features of claim 1 including the particular features discussed immediately above. Appellants essentially repeat the above argument from claim 1 for each of dependent claims 2, 3, and 5-8. Thus, it is submitted that dependent claims 2, 3, and 5-8 are allowable at least by virtue of their dependency from claim 1 and because each claim recites further distinguishing features thereover. It is respectfully requested the Board reverse the rejection of dependent claims 2, 3, and 5-8.

Claim 14

Claim 14 is an independent claim written in an apparatus form including limitations substantially similar to all the limitations discussed above in claim 1. Claim 14 calls for:

> *An arrangement for embedding a digital watermark in an information signal; the arrangement comprising*
> *- means for deriving a watermark secret from an identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert;*

- means for embedding a digital watermark in the information signal where said embedding is controlled by a watermark secret;
- means for calculating a digital fingerprint from the information signal; and
- means for storing the calculated digital fingerprint as a reference digital fingerprint and for storing, in relation to the reference digital fingerprint, a identifier data item from which the watermark secret can be derived.

Since the limitations in claim 14 are substantially identical to the method limitations in claim 1, Appellants essentially repeat the above argument from claim 1 for claim 14. Thus, it is submitted that claim 14 is allowable at least by virtue of its substantial similarity to claim 1. It is respectfully requested the Board reverse the rejection of claim 14.

2. CLAIMS 9-13 AND 15 ARE IMPROPERLY REJECTED UNDER 35 U.S.C. §103 AS BEING UNPATENTABLE OVER CONWELL IN VIEW OF DEPOVERE

Claim 9

Claim 9 is an independent method claim. Claims 10-13 depend ultimately from claim 9. Claim 15 is an apparatus claim that includes limitations substantially similar to those found in claim 9. Independent claim 9 calls, in part, for:

A method of detecting a digital watermark in an information signal; the method comprising
- providing a plurality of digital reference fingerprints each calculated from a respective reference information signal, where each digital fingerprint is associated with a corresponding watermark secret;
- calculating a digital fingerprint from the information signal;
- determining a matching digital fingerprint from the plurality of digital reference fingerprints as corresponding to the calculated digital fingerprint;
- detecting whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal.

These limitations are substantially identical to the limitations discussed above with respect to claim 1. Since the limitations in claim 9 are substantially identical to the method limitations in claim 1, Appellants essentially repeat the arguments above from claim 1 for claim 9.

Neither Conwell nor Depovere teach, show, or suggest that "each digital fingerprint is associated with a corresponding watermark secret", as defined in the claims. The present Office Action admits on pages 9 and 10 that this teaching is lacking from Conwell. Hence the Office Action points to several portion of Depovere to cure this defect in Conwell.

Depovere appears to teach the presence of a watermark payload and a secret key used for watermarking. There is no teaching, showing, or suggestion in Depovere that the watermark payload is a "digital fingerprint" as defined in claim 9. Claim 9 clearly requires that the digital

fingerprint be "calculated from a respective reference information signal, where each digital fingerprint is associated with a corresponding watermark secret", as defined in claim 9. In Depovere, the watermark payload bears to association to any part of the information signal into which it is embedded. Since Conwell also lacks any teaching or suggestion in this regard, the combination of Conwell and Depovere does not teach, show, or suggest "each calculated from a respective reference information signal, where each digital fingerprint is associated with a corresponding watermark secret", as defined in claim 9. Thus, the combination of Conwell and Depovere fail to teach all the limitations found in the claims.

For all the reasons set forth above, it is believed that the elements of claim 9 are not taught, shown, or suggested by Depovere and Conwell, either separately or in combination. It is therefore submitted that the elements of claim 9 would not have been obvious to a person of ordinary skill in the art upon a reading of Depovere and Conwell, separately or in combination. Thus, it is submitted that claim 9 is allowable under 35 U.S.C. §103. It is respectfully requested that the Board reverse this rejection of claim 9.

Dependent Claims 10-13

Claims 10-13 depend either directly or indirectly upon claim 9. Each dependent claim includes all the features of claim 9 including the particular features discussed immediately above. Appellants essentially repeat the above argument from claim 9 for each of dependent claims 10-13. Thus, it is submitted that dependent claims 10-13 are allowable at least by virtue of their dependency from claim 9 and because each claim recites further distinguishing features thereover. It is respectfully requested the Board reverse the rejection of dependent claims 10-13.

Claim 15

Claim 15 is an independent claim written in an apparatus form including limitations substantially similar to all the limitations discussed above in claim 9. Claim 15 calls for:

> *An arrangement for detecting a digital watermark in an information signal; the arrangement comprising*
> *- means for providing a plurality of digital reference fingerprints each calculated from a respective reference information signal, where each digital fingerprint is associated with a corresponding watermark secret;*
> *- means for calculating a digital fingerprint from the information signal;*
> *- means for determining a matching digital fingerprint from the plurality of digital reference fingerprints as corresponding to the calculated digital fingerprint; and*

- *means for detecting whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal.*

Since the limitations in claim 15 are substantially identical to the method limitations in claim 9, Appellants essentially repeat the above argument from claim 9 for claim 15. Thus, it is submitted that claim 15 is allowable at least by virtue of its substantial similarity to claim 9. It is respectfully requested the Board reverse the rejection of claim 15.

Conclusion

In light of these remarks, it is submitted that claims 1-3 and 5-15 would not have been obvious to a person of ordinary skill in the art upon a reading of Conwell, Depovere, and Chang, either separately or in any combination whatsoever, at the time Appellants' invention was made. Therefore, it is submitted that claims 1-3 and 5-15 are allowable under 35 U.S.C. §103. It is respectfully requested that the Board of Patent Appeals and Interferences reverse the rejection of claims 1-3 and 5-15.

Respectfully submitted,

Date: **June 22, 2009**

By: /Brian S. Myers/
Brian S. Myers
Registration No. 46,947

Please mail all correspondence to:

Corporate Counsel
US PHILIPS CORPORATION
P.O. Box 3001
Briarcliff Manor, NY 10510-8001

VIII. CLAIMS APPENDIX

1. **(Previously Presented)** A method of embedding a digital watermark in an information signal; the method comprising

- deriving a watermark secret from an identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert;
- embedding a digital watermark in the information signal where said embedding is controlled by the watermark secret;
- calculating a digital fingerprint from the information signal;
- storing the calculated digital fingerprint as a reference digital fingerprint and storing, in relation to the reference digital fingerprint, said identifier data item.

2. **(Previously Presented)** A method according to claim 1, wherein the information signal is an audio signal, the digital fingerprint is an audio fingerprint, and the digital watermark is an audio watermark.

3. **(Previously Presented)** A method according to claim 1, wherein storing the calculated digital fingerprint and said identifier data item comprises storing the calculated digital fingerprint and the identifier data item in a fingerprint database .

4. **(Cancelled)**

5. **(Previously Presented)** A method according to claim 1, wherein the watermark secret is determined by a random process.

6. **(Previously Presented)** A method according to claim 1, where the digital watermark comprises a watermark payload and wherein the watermark payload is indicative of the information signal.

7. **(Previously Presented)** A method according to claim 6, further comprising encoding said watermark payload based on an encryption key derived from an identifier indicative of an information content of the information signal.

8. **(Previously Presented)** A method according to claim 1, wherein the information signal is a video signal.

9. **(Previously Presented)** A method of detecting a digital watermark in an information signal; the method comprising

- providing a plurality of digital reference fingerprints each calculated from a respective reference information signal, where each digital fingerprint is associated with a corresponding watermark secret;
- calculating a digital fingerprint from the information signal;
- determining a matching digital fingerprint from the plurality of digital reference fingerprints as corresponding to the calculated digital fingerprint;
- detecting whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal.

10. **(Original)** A method according to claim 9, wherein determining a matching digital fingerprint comprises sending a query to a fingerprint database, the query comprising the calculated digital fingerprint; and receiving from the fingerprint database a response including a identifier data item from which the watermark secret associated with the matching digital fingerprint can be derived.

11. **(Original)** A method according to claim 10, wherein sending a query and receiving a response comprise communicating via a communications network.

12. **(Previously Presented)** A method according to claim 9, wherein the information signal comprises an encoded information signal; and calculating the digital fingerprint comprises decoding the encoded information signal, and calculating the fingerprint from the decoded information signal.

13. **(Previously Presented)** A method according to claim 10, wherein determining a matching digital fingerprint comprises performing a search in a fingerprint database based on reliability information about the calculated digital fingerprint.

14. **(Previously Presented)** An arrangement for embedding a digital watermark in an information signal; the arrangement comprising

- means for deriving a watermark secret from an identifier data item identifying the information signal by a function which is computationally hard or infeasible to invert;
- means for embedding a digital watermark in the information signal where said embedding is controlled by a watermark secret;
- means for calculating a digital fingerprint from the information signal; and
- means for storing the calculated digital fingerprint as a reference digital fingerprint and for storing, in relation to the reference digital fingerprint, a identifier data item from which the watermark secret can be derived.

15. **(Previously Presented)** An arrangement for detecting a digital watermark in an information signal; the arrangement comprising

- means for providing a plurality of digital reference fingerprints each calculated from a respective reference information signal, where each digital fingerprint is associated with a corresponding watermark secret;
- means for calculating a digital fingerprint from the information signal;
- means for determining a matching digital fingerprint from the plurality of digital reference fingerprints as corresponding to the calculated digital fingerprint; and
- means for detecting whether a digital watermark according to the watermark secret associated with the matching digital fingerprint is present in the information signal.

16. **(Cancelled)**

IX. EVIDENCE APPENDIX

No evidence has been submitted pursuant to §§ 1.130, 1.131, or 1.132 of this title. No other evidence has been entered by the Examiner and/or relied upon by Appellant in this appeal, at this time.

X. RELATED PROCEEDINGS APPENDIX

Appellants are not aware of any appeals or interferences related to the present application.